IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

STINGRAY IP SOLUTIONS LLC,	§	
	§	
v.	§	CASE NO. 2:22-cv-00420-JRG-RSP
	§	(Lead Case)
RESIDEO TECHNOLOGIES, INC., et al.	§	

STINGRAY IP SOLUTIONS LLC,	§	
	§	
Plaintiff,	§	CASE NO. 2:22-cv-00421-JRG-RSP
	§	(Member Case)
v.	§	
	§	JURY TRIAL DEMANDED
ADT INC. and ADT LLC,	§	
	§	
Defendants.	§	

PLAINTIFF'S SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Stingray IP Solutions LLC ("Stingray") files this First Amended Complaint in this Eastern District of Texas (the "District") against Defendants ADT Inc. and ADT LLC dba ADT Security Services, CAM CONNECTIONS, PROTECTION ONE and Protect Your Home (collectively, "Defendants" or "ADT") for infringement of U.S. Patent No. 7,224,678 (the "'678 patent"), U.S. Patent No. 7,440,572 (the "'572 patent"), and U.S. Patent No. 7,441,126 ("the "'126 patent").

THE PARTIES

1. Stingray IP Solutions LLC ("Stingray" or "Plaintiff") is a Texas limited liability company, located at 6136 Frisco Sq. Blvd., Suite 400, Frisco, TX 75034.

2. On information and belief, Defendant ADT Inc. is a corporation organized under the laws of Delaware, USA, with its principal place of business and corporate headquarters at 1501 Yamato Road, Boca Raton, Florida, USA 33431. ADT Inc. may be served with process via its

registered agents, including The Corporation Trust Company, Corporation Trust Center 1209 Orange St, Wilmington, DE, USA 19801. ADT Inc. is a publicly traded company on the New York Stock Exchange under the symbol "ADT."

3. On information and belief, Defendant ADT LLC is a company organized under the laws of Delaware, USA, with its principal place of business located at 1501 Yamato Road, Boca Raton, Florida, USA 33431. ADT LLC may be served with process via its registered agents, including C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX, USA 75201-3136. ADT Inc. and ADT LLC share the same location for their principal places of business. Moreover, ADT LLC is a wholly owned and controlled subsidiary of ADT Inc. ADT LLC is part of a group of companies operating under the name "ADT" of which ADT Inc. is the parent and controlling entity.

4. "ADT Inc., together with its wholly-owned subsidiaries," referred to collectively as "ADT" in ADT Inc.'s annual financial report for 2021, "is a leading provider of security, interactive, and smart home solutions serving residential, small business, and commercial customers in the United States." *See* ADT INC., *Form 10-K Annual Financial Report For the Fiscal Year Ended December 31, 2021,* p. 4, *available for download at* https://investor.adt.com/financials/sec-filings/default.aspx (last visited Oct. 6, 2022) [hereinafter "Annual Financial Report"]. In May 2016, ADT Inc. acquired The ADT Security Corporation, which significantly increased ADT's market share in the security systems industry making ADT one of the largest monitored security companies in the U.S. and, at the time, Canada. *Id.* "[ADT] primarily conducts business under the ADT brand name." *Id.* at F-10, p. 89. ADT Inc. states that "substantially all of the Company's assets are located in the U.S. as of December 31, 2021 and 2020." *Id.* at F-21, p. 100.

5. ADT's "mission is to empower customers to protect and connect to what matters most - their families, homes, and businesses - by delivering safe, smart, and sustainable lifestyle-driven solutions through professionally installed, do-it-yourself ("DIY"), and mobile or other digital-based offerings supported by our 24/7 professional monitoring services," and "[t]he ADT brand is one of the most recognized and trusted brands in the security industry, which [ADT] believe[s] is a key competitive advantage and contributor to [ADT's] success due to the importance customers place on reputation and trust when purchasing [ADT's] products and services." *Id*. ADT Inc. additionally states that "[t]he strength of [ADT's] brand is based upon a long-standing record of delivering high-quality, reliable products and services; expertise in system sales, installation, and monitoring; and superior customer care, all driven by [ADT's] industry-leading experience and knowledge." *Id*. ADT "serve[s] [its] customers through [its] nationwide sales and service offices; monitoring and support centers; and a large network of security, home-automation, and solar-installation professionals in the U.S." and "[a]s of December 31, 2021, [ADT] had approximately 6.6 million recurring revenue customers." *Id*.

6. "[ADT] ha[s] a network of over 250 sales and service offices and three regional distribution centers, which are supported by 17 multiuse sales, customer, and field support locations housing our nine UL-listed monitoring centers and four national sales centers." *Id.* ADT Inc., further states that, "[w]hile select locations may primarily support one segment or market, such as our NAOC which supports our Commercial business, these multi-use locations primarily support our business as a whole." *Id*.

7. ADT Inc. states that "[ADT] evaluate[s] and report[s] [ADT's] segment information based on the manner in which [ADT's] Chief Executive Officer, who is the chief operating decision maker (the "CODM"), evaluates performance and allocates resources." *Id.* at p. 6. "Prior

to 2021, [ADT] had a single operating and reportable segment," but "beginning in the first quarter of 2021, [ADT] reported results in two operating and reportable segments, Consumer and Small Business ("CSB") and Commercial." *Id.* "Upon consummation of the Sunpro Solar Acquisition in the fourth quarter of 2021, [ADT] began reporting results for a third operating and reportable segment related to the ADT Solar business ('Solar')." *Id.*

8. On information and belief, ADT, including parent ADT Inc. along with its subsidiaries, are engaged in research and development (including, for example, "ongoing technological innovations"), manufacturing, importation, distribution, sales, installation, servicing, monitoring and related technical services for: (i) "integrated security, interactive, and automation systems, and other related offerings," with each activity being conducted "for residential homeowners, small business operators, and other individual consumers of security and automation systems" in the United States and (ii) "integrated security, interactive, and automation systems, fire detection and suppression systems, and other related offerings" for "larger businesses with more expansive facilities (typically larger than 10,000 square feet) and multi-site operations, which often require more sophisticated integrated solutions" in the United States. *See Id.* at pp. 6-11. ADT's products are (i) manufactured outside the U.S. and then imported into the United States or (ii) manufactured inside the U.S., and distributed, and sold to end-users via the internet, brick-and-mortar stores and/or via dealers in the U.S., in Texas and the Eastern District of Texas.

9. On information and belief, ADT maintains a corporate presence in the United States, including in Texas and in this District, via at least its wholly owned and controlled U.S.-based subsidiaries, including, for example, ADT LLC dba ADT Security Services, which is a Delaware company having multiple offices in this District, including at least two offices in Tyler, Texas located at 470 DC Dr, Tyler, TX 75701 and 215 Winchester Drive, Suite 105, Tyler, TX 75701,

and a Beaumont Office located at 7415 Eastex Plaza Drive, Suite 8, Beaumont, TX 77708. *See Annual Financial Report*, Exh. 21.1 at p. 652; *Home Security Tyler*, ADT.COM, https://www.adt.com/local/tx/tyler? (last visited Oct. 5, 2022); *Home Security Beaumont*, ADT.COM, https://www.adt.com/local/tx/beaumont? (last visited Oct. 13, 2022). On behalf and for the benefit of Defendants, ADT coordinates the importation, distribution, marketing, offers for sale, sale, and use of the ADT's products in the U.S. For example, ADT maintains distribution channels in the U.S. for ADT's products via online stores, distribution partners, retailers, reseller partners, dealers, and other related service providers. *Local Home Security Monitoring in Texas*, ADT.COM, https://www.adt.com/local/tx (last visited Oct. 5, 2022); *blue by ADT*, https://www.bluebyadt.com/ (last visited Oct. 5, 2022) (offering security products, for example, smart home hub, Blue by ADT app, door/window sensors, motion sensors, mobile app, keypad, cameras, smoke detector, flood and temperature sensors, Wi-Fi range extenders, and keychain remote, under the slogan: "DIY security from ADT. Yes, that ADT.").

10. As a result, via at least ADT's established distribution channels operated and maintained by at least Defendant ADT Inc. and ADT's U.S.-based subsidiaries, including wholly owned and controlled Defendant ADT LLC, ADT products are distributed, sold, advertised, and used nationwide, including being sold to consumers via ADT dealers operating in Texas and this District. Thus, Defendants do business in the U.S., the state of Texas, and in this District.

JURISDICTION AND VENUE

11. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

A. Defendant ADT Inc.

13. On information and belief, ADT Inc. is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, subsidiaries, members, segments, companies, brands, and/or consumers. For example, ADT Inc. is related to, owns, and/or controls subsidiaries (for example, ADT LLC and The ADT Security Corporation), business segments (for example, its Consumer and Small Business ("CSB") segment and Commercial segment) and additional business and/or brands (for example, ADT, Blue by ADT, Pulse, ADT Security Services, CAM CONNECTIONS, PROTECTION ONE, Protect Your Home, brands including "ADT," and brands and registered and applied-for marks listed by the United States Patent and Trademark Office's Trademark Electronic Search System as owned by The ADT Security Corporation or ADT Holdings, Inc.) that have a significant business presence in the U.S. and in Texas. Such a presence furthers the development, design, manufacture, importation, distribution, sale, and use (including by inducement) of infringing ADT products in Texas, including in this District.

14. This Court has personal jurisdiction over Defendant ADT Inc., directly and/or through the activities of ADT Inc.'s intermediaries, agents, related entities, distributors, importers,

customers, subsidiaries, and/or consumers, including through the activities of Defendant ADT LLC, other members, segments, companies and/or brands of ADT (e.g., ADT LLC, The ADT Security Corporation, ADT Holdings, Inc., ADT, Blue by ADT, Pulse, ADT Security Services, CAM CONNECTIONS, PROTECTION ONE, Protect Your Home, brands including "ADT," and brands and registered and applied-for marks listed by the United States Patent and Trademark Office's Trademark Electronic Search System as owned by The ADT Security Corporation or ADT Holdings, Inc.), and U.S.-based subsidiaries. Through direction and control of these entities, ADT Inc. has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over ADT Inc. would not offend traditional notions of fair play and substantial justice.

15. On information and belief, ADT Inc. controls or otherwise directs and authorizes all activities of its subsidiaries and related entities, including, but not limited to Defendant ADT LLC and The ADT Security Corporation, and other members, segments, companies and/or brands of ADT. *See, e.g.*, *Home Security Tyler*, ADT.COM, https://www.adt.com/local/tx/tyler (last visited Oct. 6, 2022) (Terms of Use stating, "These ADT Website Terms and Conditions of Use (the 'Terms') govern your use [*sic*] any websites that are owned or operated by ADT LLC, d/b/a ADT Security Services ('ADT,' 'we,' 'us' or 'our'), and which contain a link to the Terms (collectively, and together with all services available through such websites, the 'Site')"); *Certification of Chief Executive Officer, Annual Financial Report*, Exh. 32.1 at p. 656; *Certification of Chief Financial Officer, Annual Financial Report*, Exh. 32.2 at p. 657; *Annual Financial Report*, F-10 at p. 89 ("[ADT] primarily conducts business under the ADT brand name."). For example, the President and Chief Executive Officer is the same for both ADT LLC and ADT Inc. *See, e.g.*, *Certification*

of Chief Executive Officer, *Annual Financial Report*, Exh. 32.1 at p. 656 (listing "James D. DeVries" as "President and Chief Executive Officer of ADT Inc."); *Management, Business Organizations Inquiry – View Entity*, DIRECT.SOS.STATE.TX.US, https://direct.sos.state.tx.us/acct/acct-login.asp (last visited Oct. 13, 2022) (via login to Texas SOSDirect, selecting menu item labeled "Business Organizations," following link entitled "Find – Entity," searching for "ADT LLC", selecting the search result for "ADT LLC" and the tab labeled "MANAGEMENT") (listing "DeVries James D" as "President and Chief Executive Of[ficer]"of ADT LLC). Directly via its agents in the U.S. and via at least distribution partners, retailers, reseller partners, dealers, professional installers, and other service providers, ADT Inc. has placed and continues to place infringing ADT products into the U.S. stream of commerce. Examples include the manufacture and/or importation of ADT products into the United States. *See, e.g.*, *Annual Financial Report*, pp. 6-11. ADT Inc. has placed such products into the stream of commerce with the knowledge and understanding that such products are, will be, and continue to be sold, offered for sale, and/or imported into this District and the State of Texas. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523 F.3d 1353, 1369-70 (Fed. Cir. 2008) ("[T]he sale [for purposes of § 271] occurred at the location of the buyer."); *see also Semcon IP Inc. v. Kyocera Corporation*, No. 2:18-cv-00197-JRG, 2019 WL 1979930, at *3 (E.D. Tex. May 3, 2019) (denying accused infringer's motion to dismiss because plaintiff sufficiently plead that purchases of infringing products outside of the United States for importation into and sales to end users in the U.S. may constitute an offer to sell under § 271(a)).

16. On information and belief, ADT utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including providing links via its own website to online stores, retailers,

detailers, resellers, distributors, and dealers offering such products and related services for sale. *See ADT Security Local Service Areas*, ADT.COM, https://www.adt.com/local (last visited Oct. 6, 2022); *blue by ADT*, BLUEBYADT.COM, https://www.bluebyadt.com/ (last visited Oct. 6, 2022); *ADT OUTDOOR CAMERA PRO 1080P*, ZIONSSECURITY.COM, https://zionssecurity.com/product/adt-outdoor-camera-pro-1080p/ (last visited Oct. 6, 2022) ("The ADT Outdoor Camera Pro 1080P is perfect if you want to see your driveway or backyard from your ADT app. It works with both the Pulse and Control app. It is a weatherproof, infrared, WiFi camera with 1080P HD Quality Video!"). Such ADT products and/or services have been sold from and/or in both brick-and-mortar and/or online retail stores within this District and in Texas, with examples being ADT Security Services offices located in Tyler, Texas, an ADT Security Services Office located in Beaumont, Texas, locations listed on the ADT website, nationwide dealers or distributors, and at least one nationwide online retailer or online retail store. *See, e.g.*, *Home Security Tyler*, ADT.COM, https://www.adt.com/local/tx/tyler? (last visited Oct. 5, 2022); *Home Security Beaumont*, ADT.COM, https://www.adt.com/local/tx/beaumont? (last visited Oct. 13, 2022); *blue by ADT*, BLUEBYADT.COM, https://www.bluebyadt.com/ (last visited Oct. 6, 2022); *ADT OUTDOOR CAMERA PRO 1080P*, ZIONSSECURITY.COM, https://zionssecurity.com/product/adt-outdoor-camera-pro-1080p/ (last visited Oct. 6, 2022). Additionally, ADT products, including infringing products and/or services, are and have been sold nationwide, in Texas and this District via, for example, direct sales, at least one online retail store, and dealers. *See, e.g.*, *ADT Doorbell Camera*, ADT.COM, https://www.adt.com/doorbell-camera (last visited Oct. 6, 2022); *Outdoor Security Cameras*, ADT.COM, https://www.adt.com/outdoor-security-camera (last visited Oct. 6, 2022) ("Only requires a power source and Wi-Fi connection."); *Indoor Security Cameras*, ADT.COM, https://www.adt.com/indoor-security-camera

(last visited Oct. 6, 2022) ("Place indoor cameras anywhere in your home within Wi-Fi signal range of the control panel."); *ADT Command*, ADT.COM, https://www.adt.com/command (last visited Oct. 6, 2022); *How to configure Wi-Fi on your ADT Command panel*, YOUTUBE.COM, https://www.youtube.com/watch?v=ZjNP95AeMZ4 (last visited Oct. 6, 2022); *Smart Home*, ADT.COM, https://www.adt.com/shop/packages/smart-home.html (last visited Oct. 6, 2022) (showing the Secondary Wireless Touchscreen has a "Wi-Fi" frequency of operation); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 6, 2022) ("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access."); *Wireless Outdoor Camera*, BLUEBYADT.COM, https://www.bluebyadt.com/shop/blue-outdoor-camera.html (last visited Oct. 6, 2022); *Blue by ADT Doorbell Camera*, SUPPORT.BLUEBYADT.COM, https://support.bluebyadt.com/s/article/Blue-by-ADT-Doorbell-Cameras (last visited Oct. 6, 2022). ADT wireless security cameras are offered for sale in this District at least via ADT Security Services Offices at 4706 DC Dr, Tyler, TX 75701, at 215 Winchester Drive, Suite 105, Tyler, TX 75701, and at 7415 Eastex Plaza Drive, Suite 8, Beaumont, TX 77708, and online at least by bluebyadt.com. *See, e.g.*, *Home Security Tyler*, ADT.COM, https://www.adt.com/local/tx/tyler? (last visited Oct. 5, 2022); *Home Security Beaumont*, ADT.COM, https://www.adt.com/local/tx/beaumont? (last visited Oct. 13, 2022); *blue by ADT*, BLUEBYADT.COM, https://www.bluebyadt.com/ (last visited Oct. 6, 2022); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 6, 2022) ("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access."). ADT Inc., via its wholly owned and controlled subsidiaries, also provides application software

("apps") for download and use in conjunction with and as a part of the wireless communication network that connects ADT products and other network devices. *See, e.g., Apps for your mobile lifestyle*, ADT.COM, https://www.adt.com/apps (last visited Oct. 6, 2022) (showing ADT SoSecure app, ADT Control app, and noting integration of Google Assistant-enabled Google Nest Mini with the ADT system enables voice commands of security, locks, lights, music and more); *ADT PULSE APP*, ADT.COM, https://www.adt.com/pulse (last visited Oct. 6, 2022). These apps are available via digital distribution platforms operated, for example, by Apple Inc. and Google for download by users and execution on smartphone devices. *See, e.g., Apps for your mobile lifestyle,* ADT.COM, https://www.adt.com/apps (last visited Oct. 6, 2022) ("Download the free app from the Apple or Google Play Store.").

17. Based on ADT Inc.'s connections and relationship with manufacturers, dealers, retailers, and digital distribution platforms, ADT Inc. knows that Texas is a termination point of the established distribution channel, namely online and brick-and-mortar stores offering ADT products and related services and software to third-party manufacturers, distribution partners, retailers (including national retailers), reseller partners, dealers, service providers, consumers, and other users in Texas. ADT Inc., therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought into this Court, at least on this basis. *See Icon Health & Fitness, Inc. v. Horizon Fitness, Inc.*, 2009 WL 1025467, at (E.D. Tex. 2009) (finding that "[a]s a result of contracting to manufacture products for sale in" national retailers' stores, the defendant "could have expected that it could be brought into court in the states where [the national retailers] are located").

18. On information and belief, ADT Inc. alone and in concert with other related entities such as Defendant ADT LLC, and subsidiaries, and members, segments, companies and/or brands

of ADT, manufactures and purposefully places infringing ADT products in established distribution channels in the stream of commerce, including in Texas, via third-party manufacturers, distributors, dealers, and reseller partners, such as at least those operating online and/or those listed on ADT's website. As an example, ADT Inc. manufactures ADT products in Texas and/or imports ADT products to Texas directly and/or through a related entity or subsidiary and directly sells and offers for sale infringing ADT products in Texas to resellers or dealers. For example, ADT products including at least smart home and video packages are offered for sale at ADT Security Services offices and/or authorized providers located in this District in McKinney, TX, for example, at 1720 N Central Expy, McKinney, TX 75070. *See, e.g., SafeStreets*, HOMESCURITYSMITH.COM, https://homesecuritysmith.com/adt-security-locations/texas/mckinney-tx/ (last visited Oct. 6, 2022) (offering individually customized & installed packages "From basic packages to smart home and video remote monitoring" via ADT Authorized Provider Safe Streets USA); *McKinney TX, ADT® Home Security Deals and Alarm System Specials*, HOMESALARM.COM, https://www.homesalarm.com/texas/adt-mckinney-tx/ (last visited Oct. 6, 2022) (offering professionally customized & installed "Smart home security and video packages" via Homesalarm.com); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 6, 2022) ("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access."). These suppliers, distributors, dealers, and/or resellers import, advertise, offer for sale and/or sell ADT products and/or related services, such as consultation and installation, via their own websites to U.S. consumers, including to consumers in Texas and this District. Based on ADT Inc.'s connections and relationship, including supply contracts and other agreements with the U.S.- and Texas-based suppliers, distributors, dealers,

and/or resellers, such as at least Safe Streets USA, ADT Inc. knows and has known that Texas is a termination point of the established distribution channels for ADT products. ADT Inc., alone and in concert with subsidiaries Defendant ADT LLC, and U.S.-based Members, segments, companies and/or brands of ADT has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this additional basis. *See Ultravision Technologies, LLC v. Holophane Europe Limited*, 2020 WL 3493626, at *5 (E.D. Tex. 2020) (finding sufficient to make a *prima facie* showing of personal jurisdiction allegations that "Defendants either import the products to Texas themselves or through a related entity"); *see also Bench Walk Lighting LLC v. LG Innotek Co., Ltd et al.*, Civil Action No. 20-51-RGA, 2021 WL 65071, at *7-8 (D. Del., Jan. 7, 2021) (denying motion to dismiss for lack of personal jurisdiction based on the foreign defendant entering into supply contract with U.S. distributor and the distributor sold and shipped defendant's products from the U.S. to the a customer in the forum state).

19. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant ADT Inc. has committed acts of infringement in this District. As further alleged herein, Defendant ADT Inc., via its own operations and/or employees, has a regular and established place of business in this District, for example, in Smith County, at 4706 DC Dr, Tyler, TX 75701, at 215 Winchester Drive, Suite 105, Tyler, TX 75701, and in Jefferson County, at 7415 Eastex Plaza Drive, Suite 8, Beaumont, TX 77708, among other ADT locations owned, leased and/or operated in this District. Accordingly, ADT Inc. may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant ADT LLC

20. On information and belief, Defendant ADT LLC is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due

at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its partners, alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, ADT LLC and parent Defendant ADT Inc. and ADT Inc.'s U.S.-based subsidiaries, and members, segments, companies and/or brands of ADT manufacture, import, distribute, offer for sale, sell, and induce infringing use of ADT products to distribution partners, retailers (including national retailers), resellers, dealers, service providers, consumers, and other users.

21. On information and belief, this Court has personal jurisdiction over ADT LLC, directly and/or indirectly via the activities of ADT LLC's intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including parent Defendant ADT Inc. and U.S.-based subsidiaries, and members, segments, companies and/or brands of ADT.

22. On information and belief, ADT LLC utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including offering such products and/or related services for sale. ADT products and services have been sold from and/or in both brick-and-mortar stores and online retail stores by entities within this District and in Texas. Alone and in concert with or via direction and control of or by at least these entities, ADT LLC has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or

has established minimum contacts with Texas. For example, ADT LLC operates within a global network of manufacturing, sales and distribution of ADT products that includes subsidiaries of ADT Inc., retail stores, showrooms, dealers, resellers, professional installers, and/or distributors operating in Texas, including this District.

23. As another example, on information and belief, ADT LLC maintains an office in this District through at least brick-and-mortar locations at 4706 DC Dr, Tyler, TX 75701, at 215 Winchester Drive, Suite 105, Tyler, TX 75701, and at 7415 Eastex Plaza Drive, Suite 8, Beaumont, TX 77708. *See., e.g., See, e.g., Home Security Tyler, ADT.COM, https://www.adt.com/local/tx/tyler? (last visited Oct. 5, 2022); Home Security Beaumont, ADT.COM, https://www.adt.com/local/tx/beaumont?* (last visited Oct. 13, 2022)*; Account Number 40100151332000 Tax Year 2022*, SMITH CAD, https://www.smithcad.org/Search/PropertySearch.html (showing that "ADT LLC" owns property located at 4706 DC DR, Tyler, TX); *Property ID: 325677 For Year 2022*, JEFFERSON CAD, https://esearch.jcad.org/Property/View/325677 (showing that "ADT LLC" owns property located in Beaumont, TX).

24. On information and belief, as a part of ADT's global manufacturing and distribution network, ADT LLC also purposefully places infringing ADT products in established distribution channels in the stream of commerce, including in Texas, via distribution partners, retailers (including national retailers), resellers, dealers, brand ambassadors, service providers, consumers, and other users. *See, e.g., Home Security Tyler*, ADT.COM, https://www.adt.com/local/tx/tyler? (last visited Oct. 5, 2022); *Home Security Beaumont*, ADT.COM, https://www.adt.com/local/tx/beaumont? (last visited Oct. 13, 2022); *blue by ADT*, BLUEBYADT.COM, https://www.bluebyadt.com/ (last visited Oct. 6, 2022); *ADT OUTDOOR*

CAMERA PRO 1080P, ZIONSSECURITY.COM, https://zionssecurity.com/product/adt-outdoor-camera-pro-1080p/ (last visited Oct. 6, 2020) ("The ADT Outdoor Camera Pro 1080P is perfect if you want to see your driveway or backyard from your ADT app. It works with both the Pulse and Control app. It is a weatherproof, infrared, WiFi camera with 1080P HD Quality Video!"); *SafeStreets*, HOMESCURITYSMITH.COM, https://homesecuritysmith.com/adt-security-locations/texas/mckinney-tx/ (last visited Oct. 6, 2022) (offering individually customized & installed packages "From basic packages to smart home and video remote monitoring" via ADT Authorized Provider Safe Streets USA); *McKinney TX, ADT® Home Security Deals and Alarm System Specials*, HOMESALARM.COM, https://www.homesalarm.com/texas/adt-mckinney-tx/ (last visited Oct. 6, 2022) (offering professionally customized & installed "Smart home security and video packages" via Homesalarm.com); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 6, 2022) ("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access."). For example, ADT LLC provides infringing ADT product under the ADT brand and blue by ADT brand. Furthermore, ADT wireless doorbell cameras, outdoor security cameras, indoor security cameras, ADT command panels, and touchscreens are offered for sale in this District by at least ADT's local offices and/or nationwide online retail stores, for example, at adt.com and bluebyadt.com. *See, e.g.*, *ADT Doorbell Camera*, ADT.COM, https://www.adt.com/doorbell-camera (last visited Oct. 6, 2022); *Outdoor Security Cameras*, ADT.COM, https://www.adt.com/outdoor-security-camera (last visited Oct. 6, 2022) ("Only requires a power source and Wi-Fi connection."); *Indoor Security Cameras*, ADT.COM, https://www.adt.com/indoor-security-camera (last visited Oct. 6, 2022) ("Place indoor cameras anywhere in your home within Wi-Fi signal range of the control panel."); *ADT Command*,

ADT.COM, https://www.adt.com/command (last visited Oct. 6, 2022); *How to configure Wi-Fi on your ADT Command panel*, YOUTUBE.COM, https://www.youtube.com/watch?v=ZjNP95AeMZ4 (last visited Oct. 6, 2022); *Smart Home*, ADT.COM, https://www.adt.com/shop/packages/smart-home.html (last visited Oct. 6, 2022) (showing the Secondary Wireless Touchscreen has a "Wi-Fi" frequency of operation); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 6, 2022) ("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access."); *Wireless Outdoor Camera*, BLUEBYADT.COM, https://www.bluebyadt.com/shop/blue-outdoor-camera.html (last visited Oct. 6, 2022); *Blue by ADT Doorbell Camera*, SUPPORT.BLUEBYADT.COM, https://support.bluebyadt.com/s/article/Blue-by-ADT-Doorbell-Cameras (last visited Oct. 6, 2022). Additionally, ADT LLC owns and operates websites for ADT that offer products and services to consumers in the United States, in Texas, and in this District. *See, e.g., Home Security Tyler*, ADT.COM, https://www.adt.com/local/tx/tyler (last visited Oct. 6, 2022) (Terms of Use stating, "These ADT Website Terms and Conditions of Use (the 'Terms') govern your use [*sic*] any websites that are owned or operated by ADT LLC, d/b/a ADT Security Services ('ADT,' 'we,' 'us' or 'our'), and which contain a link to the Terms (collectively, and together with all services available through such websites, the 'Site')"); *Terms of Service*, BLUEBYADT.COM, https://www.bluebyadt.com/legal/terms-of-service/ (last visited Oct. 13, 2022) ("This Agreement (the 'Agreement') is made by and between ADT LLC ('ADT') and You ('Customer'). In this Agreement, Customer is sometimes referred to herein as 'you' or 'your' and the terms 'we', 'us', or 'our' means ADT and any of ADT's parents, subsidiaries, partners, related parties, employees, subcontractors, assignees or others that we hire to help us deliver the products and services we

provide to you under this Agreement.") Therefore, ADT LLC, alone and in concert with other members, segments, companies and/or brands of ADT, its parent entity Defendant ADT Inc. and its U.S.-based ADT subsidiaries has purposefully directed its activities at Texas, and should reasonably anticipate being brought into this Court, at least on this basis. Through its own conduct and through direction and control of its subsidiaries or control by other Defendant ADT Inc., ADT LLC has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over ADT LLC would not offend traditional notions of fair play and substantial justice.

25. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant ADT LLC has committed acts of infringement in this District. As further alleged herein, Defendant ADT LLC, via its own operations and/or employees, has a regular and established place of business in this District, for example, in Smith County, at 4706 DC Dr, Tyler, TX 75701, at 215 Winchester Drive, Suite 105, Tyler, TX 75701, and in Jefferson County, at 7415 Eastex Plaza Drive, Suite 8, Beaumont, TX 77708, among other ADT locations owned, leased and/or operated in this District. Accordingly, ADT LLC may be sued in this district under 28 U.S.C. § 1400(b).

26. On information and belief, Defendants ADT Inc. and ADT LLC each have significant ties to, and presence in, the State of Texas and this District, making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

27. The Asserted Patents cover various aspects of monitoring, detecting intrusions, and encrypting and decrypting wireless communications networks, including networks created between Defendants' smart home devices.

28. The ’678 patent involves detecting intrusions into a wireless local or metropolitan area network. The disclosed intrusion detection techniques include monitoring transmission between stations of the network, where each station has its own media access layer (MAC) address. The monitoring is done to detect failed attempts to authenticate the MAC addresses. Upon detection of a number of failed attempts to authenticate, an intrusion alert may be generated.

29. The ’572 patent involves providing secure wireless local area networks (LAN). A device for securing such a LAN may include a housing with a wireless transceiver carried by the housing. A medium access controller (MAC) is also carried by the housing. A cryptography circuit may be connected to the MAC controller and the transceiver. The circuit may encrypt both address and data information by at least adding a plurality of encrypting bits to be transmitted. And the cryptography circuit may decrypt both address and data information upon reception.

30. The ’126 patent provides a secure wireless local area network (LAN) utilizing a LAN device. This device may include a housing that carries a wireless transceiver and, a media access controller (MAC). A cryptography circuit carried by the housing may be connected to the MAC and the wireless transceiver. And the cryptography circuit may comprise a volatile memory provided for storing cryptography information and may also comprise a battery provided for maintaining the cryptography information stored on the volatile memory.

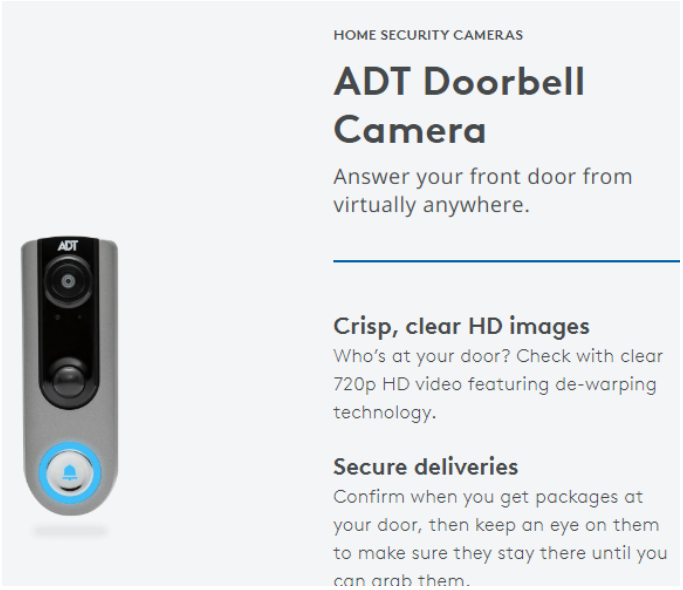
31. On information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture, distribution, sale, servicing, installation and/or use of home and business networking, IoT, and smart home products and components, which are manufactured in or imported into the United States, distributed to resellers, dealers, and third-party manufacturers, and ultimately sold to and used by U.S. consumers. For example, ADT reported that its CSB segment had 4,146,023 thousand dollars (4.146 billion U.S. dollars) in revenue and

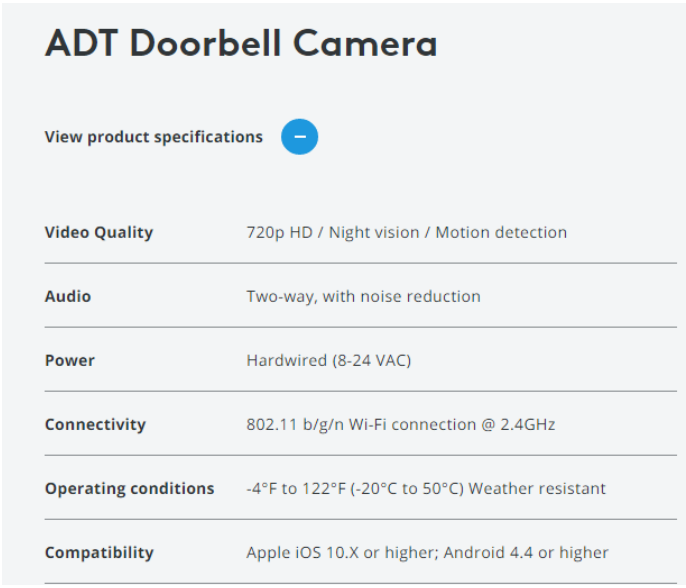
its Commercial segment had 1,113,732 thousand dollars (1.114 billion U.S. dollars) in the year ended December 31, 2021. *See Annual Financial Report,* F-17 at p. 96.

32. The Asserted Patents cover Defendants' home and business IoT and smart home products and components, software, services, and processes related to same that generally connect to other devices in a network or other networks using a wireless protocol, such as Wi-Fi. *See, e.g.*, *Smart Home*, ADT.COM, https://www.adt.com/shop/packages/smart-home.html (last visited Oct. 7, 2022) ("Some features, including mobile notifications, remote control, video streaming, and video recording require working internet and Wi-Fi."); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 6, 2022) ("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access."). Defendants' infringing ADT products include, but are not limited to, devices and products enabled or compliant with Wi-Fi, including without limitation ADT and/or Blue by ADT Doorbell Cameras; Outdoor Security Cameras; Indoor Security Cameras; Command Panels; Wireless Touchscreen Panels (e.g., Secondary Wireless Touchscreen); smartphone and/or tablet applications (e.g., ADT SoSecure, ADT Control, and ADT Pulse apps); ADT packages (e.g., ADT Smart Home packages) that include any of these products; and related accessories and software (all collectively referred to as the "Accused Products"). These Accused Products infringe the Asserted Patents by at least their manufacture, importation, distribution, sale, and use in the U.S.

33. The Asserted Patents cover Accused Products of ADT that utilize the Wi-Fi protocol. Examples of such products include ADT Doorbell Cameras, ADT Outdoor Security Cameras, ADT Indoor Security Cameras, ADT Command Panels, ADT Secondary Wireless Touchscreens, Blue by ADT Doorbell Cameras, Blue by ADT Wireless Indoor Cameras, and Blue by ADT

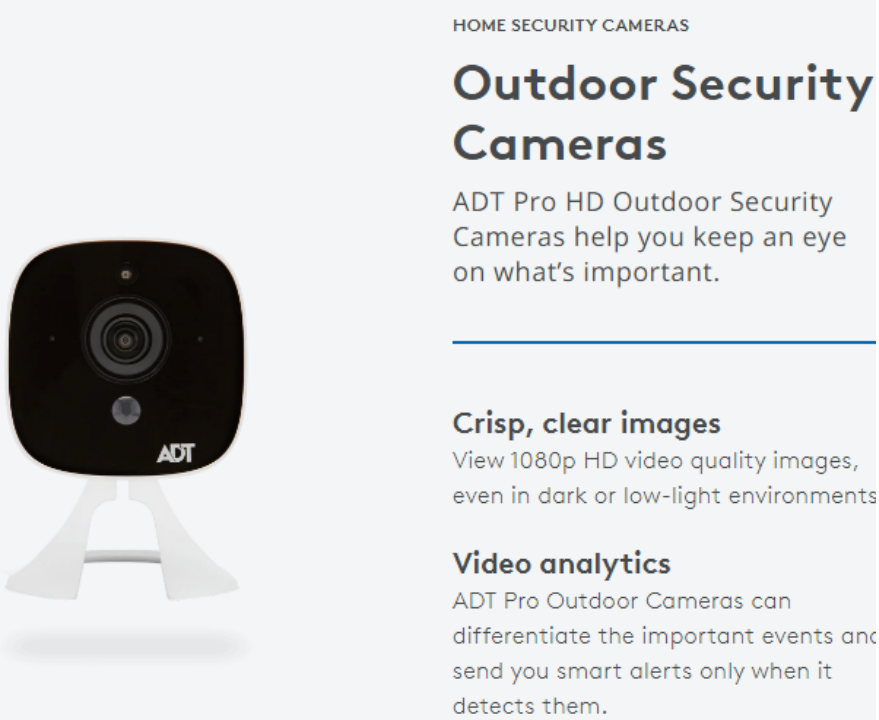
Wireless Outdoor Cameras. As shown below, the ADT Doorbell Cameras, ADT Outdoor Security Cameras, ADT Indoor Security Cameras, ADT Command Panels, ADT Secondary Wireless Touchscreens, Blue by ADT Doorbell Cameras, Blue by ADT Wireless Outdoor Cameras, and Blue by ADT Indoor Cameras are Wi-Fi (IEEE 802.11) compliant:





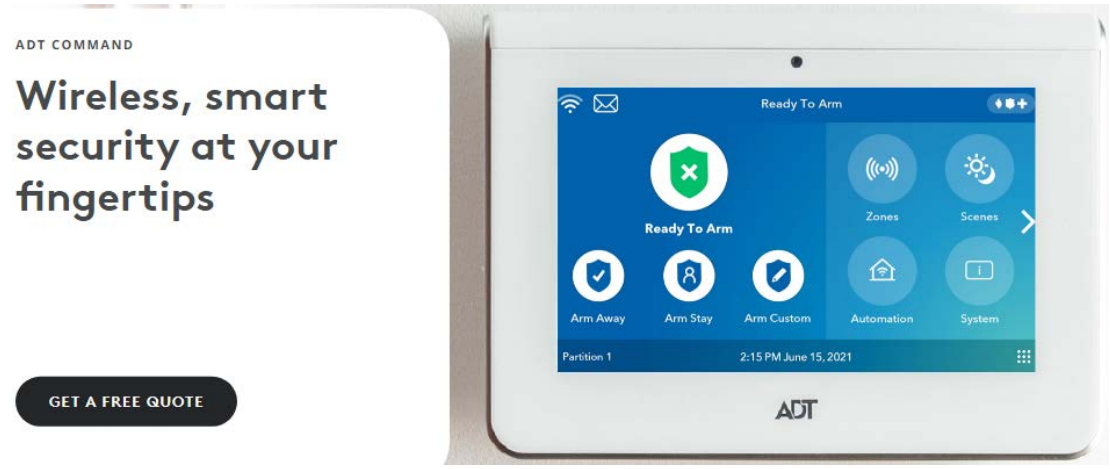
ADT Doorbell Camera, ADT.COM, https://www.adt.com/doorbell-camera (last visited Oct. 7, 2022); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 7, 2022)

("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access.").

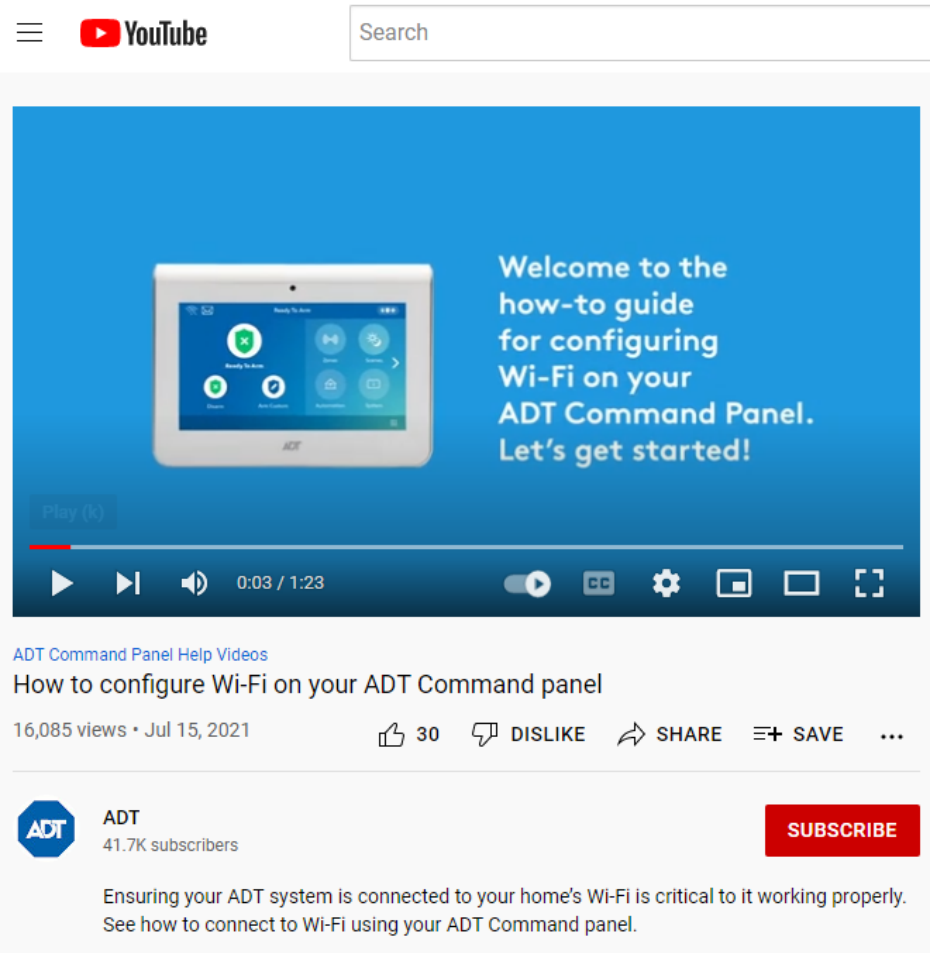


Outdoor Security Cameras, ADT.COM, https://www.adt.com/outdoor-security-camera (last visited Oct. 7, 2022) ("Only requires a power source and Wi-Fi connection."); *What Are Wireless Security Cameras, and Do I Need One?*, ADT.COM, https://www.adt.com/resources/what-are-wireless-security-cameras (last visited Oct. 7, 2022) ("ADT cameras use an encrypted wireless protocol known as WPA2, an industry-recognized method to limit wireless network access.").

Indoor Security Cameras, ADT.COM, https://www.adt.com/indoor-security-camera (last visited Oct. 6, 2022) ("Place indoor cameras anywhere in your home within Wi-Fi signal range of the control panel.").



ADT Command, ADT.COM, https://www.adt.com/command (last visited Oct. 7, 2022);



How to configure Wi-Fi on your ADT Command panel, YOUTUBE.COM, https://www.youtube.com/watch?v=ZjNP95AeMZ4 (last visited Oct. 7, 2022).

Secondary Wireless Touchscreen

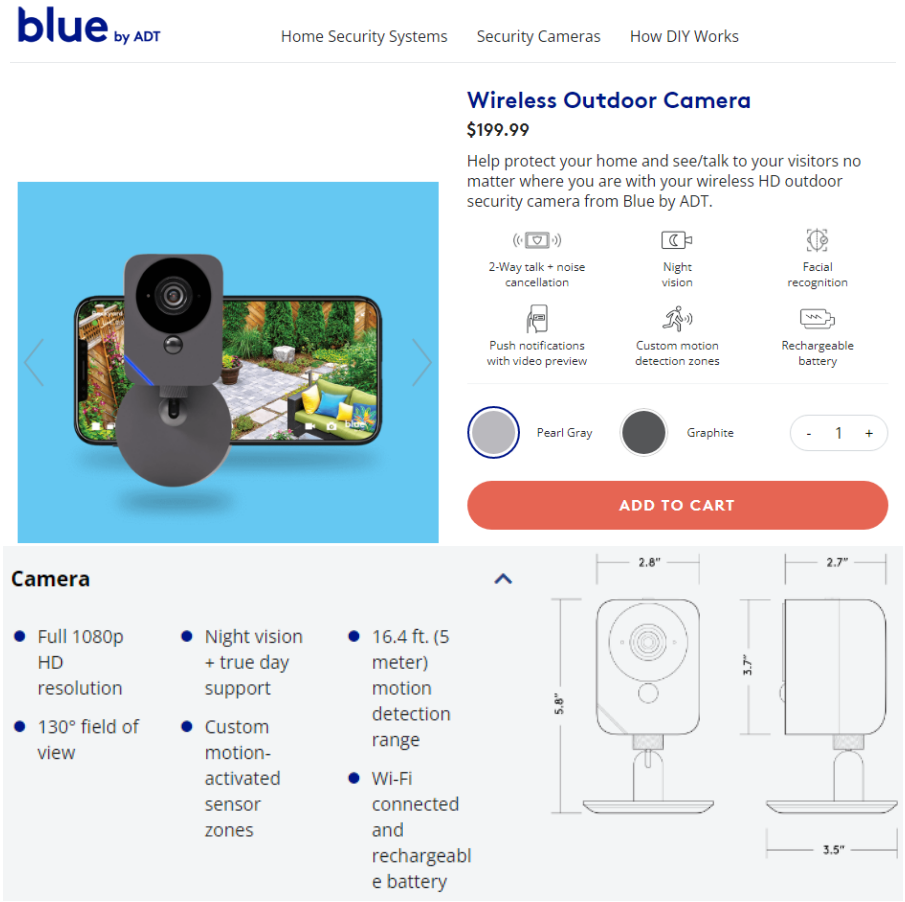
OVERVIEW

FEATURES

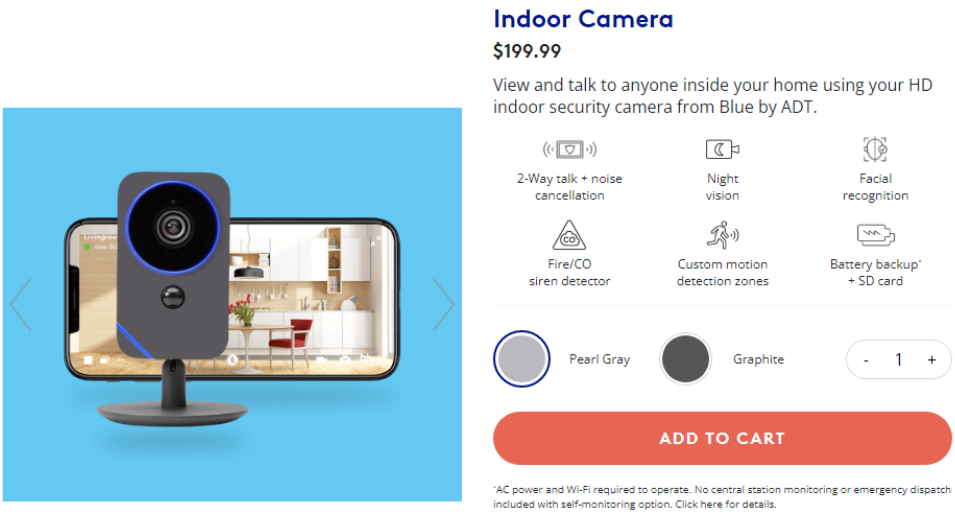
SPECIFICATIONS

Dimensions (W x H x D)	7.68" W x 4.76" H x 0.708" D (195mm x 121mm x 18mm)
Frequency of operation	Wi-Fi

Smart Home, ADT.COM, https://www.adt.com/shop/packages/smart-home.html (last visited Oct. 7, 2022) (showing the Secondary Wireless Touchscreen has a "Wi-Fi" frequency of operation).



Wireless Outdoor Camera, BLUEBYADT.COM, https://www.bluebyadt.com/shop/blue-outdoor-camera.html (last visited Oct. 7, 2022).



Indoor Camera, BLUEBYADT.COM, https://www.bluebyadt.com/shop/blue-indoor-camera.html (last visited Oct. 7, 2022); *Cameras & Devices*, BLUEBYADT.COM, https://www.bluebyadt.com/shop/blue-security-cameras/ (last visited Oct. 7, 2022) ("All Blue by

ADT cameras communicate via Wi-Fi and require an internet connection with a minimum bandwidth of 2 Mbps or higher. You will also need a mobile device with the latest iOS or Android OS.").

Blue by ADT Doorbell Camera, SUPPORT.BLUEBYADT.COM, https://support.bluebyadt.com/s/article/Blue-by-ADT-Doorbell-Cameras (last visited Oct. 7, 2022).

34. The Accused Products utilize intrusion detection methods for a local or metropolitan area network to infringe at least the '678, '572, and '126 patents. For example, the IEEE 802.11 authentication methods utilized by the Accused Products include a TKIP-based method, as explained below, that uses a "MIC" to defend against active attacks.

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

— Bit-flipping attacks
— Data (payload) truncation, concatenation, and splicing
— Fragmentation attacks
— Iterative guessing attacks against the key
— Redirection by modifying the MPDU DA or RA field
— Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

35. Stations (STAs) in an IEEE 802.11 network of the Accused Products associate with each other using a robust security network association (RSNA). As described below, RSNA supports intrusion detection by employing authentication mechanisms and data frame protection mechanisms (such as, temporal key integrity protocol - TKIP) between the STAs. Data is exchanged between the STAs in the form of MPDUs (medium access control (MAC) protocol data units). The MAC frame (MPDU) comprises a MSDU (information frame) in the frame body, and

four addresses that identify, among others, source MAC address (SA) and destination MAC address (DA) for the MSDU.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

5.1.1.4 Interaction with other IEEE 802® layers

IEEE Std 802.11 is required to appear to higher layers [logical link control (LLC)] as a wired IEEE 802 LAN. This requires that the IEEE 802.11 network handle STA mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE Std 802.11 to incorporate functionality that is untraditional for MAC sublayers.

In a robust security network association (RSNA), IEEE Std 802.11 provides functions to protect data frames, IEEE Std 802.1X-2004 provides authentication and a Controlled Port, and IEEE Std 802.11 and IEEE Std 802.1X-2004 collaborate to provide key management. All STAs in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This standard defines how an RSNA utilizes IEEE Std 802.1X-2004 to access these services.

3.126 robust security network (RSN): A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN information element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

3.127 robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of an RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

5.2.3.2 RSNA

An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

- Enhanced authentication mechanisms for STAs
- Key management algorithms
- Cryptographic key establishment
- An enhanced data cryptographic encapsulation mechanism, called Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP).

Page 72, 61, 75 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

36. In the TKIP protocol of the Accused Products, an MSDU transmitter STA calculates cryptographic message integrity code (MIC) using the MAC addresses (SA & DA) corresponding to the MSDU. As described below, the transmission is monitored if the MIC (which is obtained

using the MAC addresses) is verified/authenticated at the receiver. MSDUs with invalid MICs are discarded and countermeasures are invoked.

8.3 RSNA data confidentiality protocols

8.3.1 Overview

This standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP. Implementation of CCMP shall be mandatory in all IEEE 802.11 devices claiming RSNA compliance. Implementation of TKIP is optional for an RSNA. A design aim for TKIP was that the algorithm should be implementable within the capabilities of most devices supporting only WEP, so that many such devices would be field-upgradeable by the supplier to support TKIP.

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1 TKIP overview

The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP as follows:

a) A transmitter calculates a keyed cryptographic message integrity code (MIC) over the MSDU SA and DA, the MSDU priority (see 8.3.2.3), and the MSDU plaintext data. TKIP appends the computed MIC to the MSDU data prior to fragmentation into MPDUs. The receiver verifies the MIC after decryption, ICV checking, and defragmentation of the MPDUs into an MSDU and discards any received MSDUs with invalid MICs. TKIP's MIC provides a defense against forgery attacks.

b) Because of the design constraints of the TKIP MIC, it is still possible for an adversary to compromise message integrity; therefore, TKIP also implements countermeasures. The countermeasures bound the probability of a successful forgery and the amount of information an attacker can learn about a key.

Page 213, 214 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

37. The TKIP MIC implementation of the Accused Products prevents intrusion attacks, such as, message redirection by modifying destination/receiver MAC address (DA or RA) and impersonation by modifying the source/transmitter MAC address (SA or TA). As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is verified/authenticated at the receiver. MSDU with an invalid MIC will indicate a modified MAC address (SA or DA), thereby resulting in discarding the MSDU and invoking the countermeasures.

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

- Bit-flipping attacks
- Data (payload) truncation, concatenation, and splicing
- Fragmentation attacks
- Iterative guessing attacks against the key
- Redirection by modifying the MPDU DA or RA field
- Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

38. Upon detecting a first MIC failure, as described below, a countermeasure timer is initiated, and a failure event (alert) is reported to the AP by sending a Michael MIC Failure Report frame. Upon detecting a second consecutive MIC failure within 60 seconds, i.e., detecting a number of failed attempts, the participating STAs are deauthenticated, wherein deauthentication involves sending a notification (i.e., generating an alert) to deauthenticate due to an intrusion (2 consecutive MIC failures has occurred).

8.3.2.4 TKIP countermeasures procedures

The TKIP MIC trades off security in favor of implementability on pre-RSNA devices. Michael provides only weak protection against active attacks. A failure of the MIC in a received MSDU indicates a probable active attack. A successful attack against the MIC would mean an attacker could inject forged data frames and perform further effective attacks against the encryption key itself. If TKIP implementation detects a probable active attack, TKIP shall take countermeasures as specified in this subclause. These countermeasures accomplish the following goals:

— MIC failure events *should* be logged as a security-relevant matter. A MIC failure is an almost certain indication of an active attack and warrants a follow-up by the system administrator.

— The rate of MIC failures *must* be kept below two per minute. This implies that STAs and APs detecting two MIC failure events within 60 s must disable all receptions using TKIP for a period of 60 s. The slowdown makes it difficult for an attacker to make a large number of forgery attempts in a short time.

A single counter or timer shall be used to log MIC failure events. These failure events are defined as follows:

— For an Authenticator:
  — Detection of a MIC failure on a received unicast frame.
  — Receipt of Michael MIC Failure Report frame.
— For a Supplicant:
  — Detection of a MIC failure on a received unicast or broadcast/multicast frame.
  — Attempt to transmit a Michael MIC Failure Report frame.

The number of MIC failures is accrued independent of the particular key context. Any single MIC failure, whether detected by the Supplicant or the Authenticator and whether resulting from a group MIC key failure or a pairwise MIC key failure, shall be treated as cause for a MIC failure event.

The Supplicant uses a single Michael MIC Failure Report frame to report a MIC failure event to the Authenticator. A Michael MIC Failure Report is an EAPOL-Key frame with the following Key Information

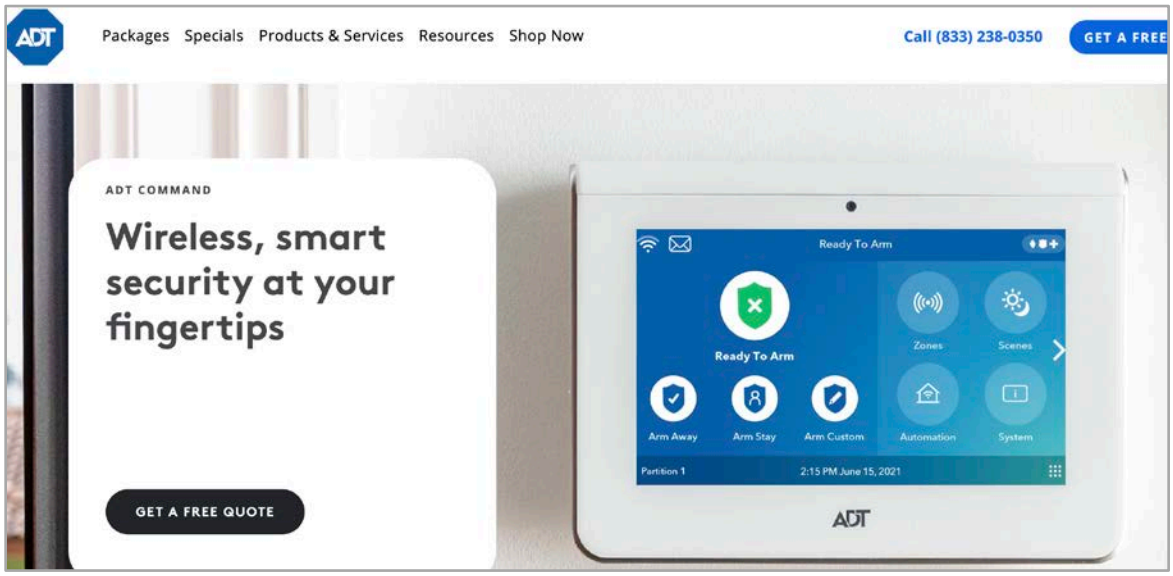
The first MIC failure shall be logged, and a timer initiated to enable enforcement of the countermeasures. If the MIC failure event is detected by the Supplicant, it shall also report the event to the AP by sending a Michael MIC Failure Report frame.

If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator. For an IBSS STA, both Supplicant and Authenticator actions shall be taken. Furthermore, the device shall not receive or transmit any TKIP-encrypted data frames, and shall not receive or transmit any unencrypted data frames other than IEEE 802.1X messages, to or from any peer for a period of at least 60 s after it detects the second failure. If the device is an AP, it shall disallow new associations using TKIP during this 60 s period; at the

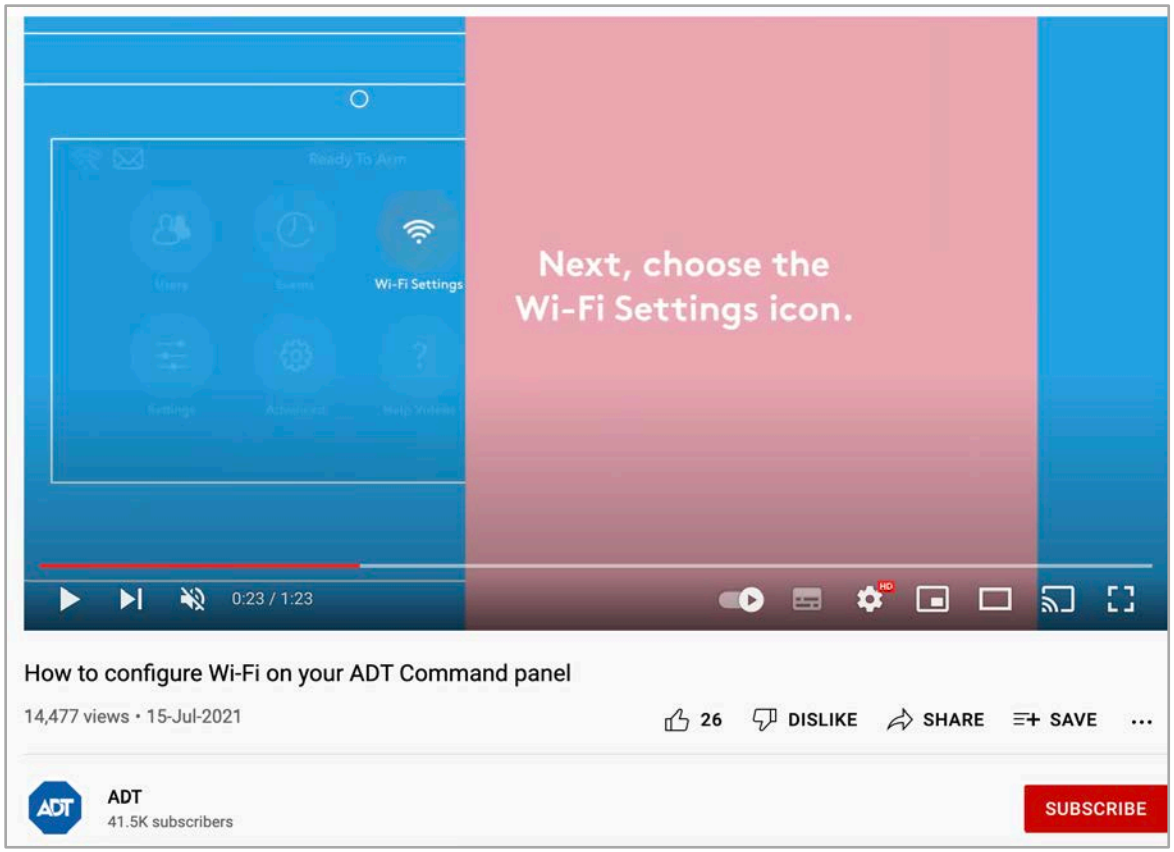
Page 219, 220, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

39. The Asserted Patents also cover ADT's Wi-Fi compliant devices, which support WPA, WPA2, and/or WPA3 security mechanisms, as described below and in the following paragraph. Of the WPA, WPA2 and/or WPA3 security mechanism used by the Accused Products, for example, ADT's smart home Wi-Fi devices, the WPA is based on Temporal Key Integrity

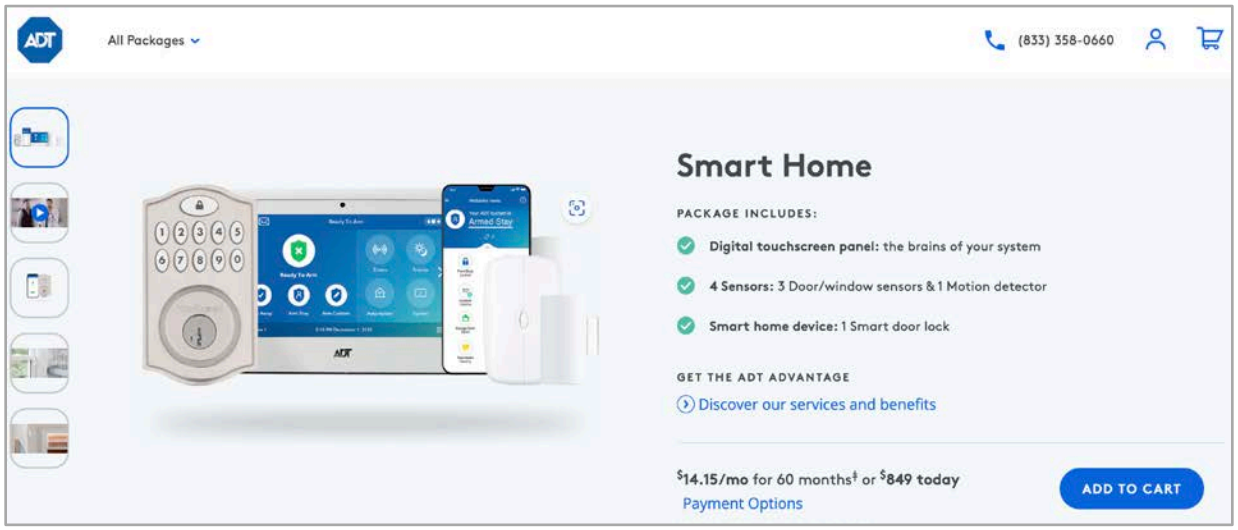
Protocol (TKIP), while the WPA2 and WPA3 are based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below are exemplary IEEE 802.11 compliant smart command panels and smart home packages that include a secondary wireless touchscreen. The devices each have a housing.

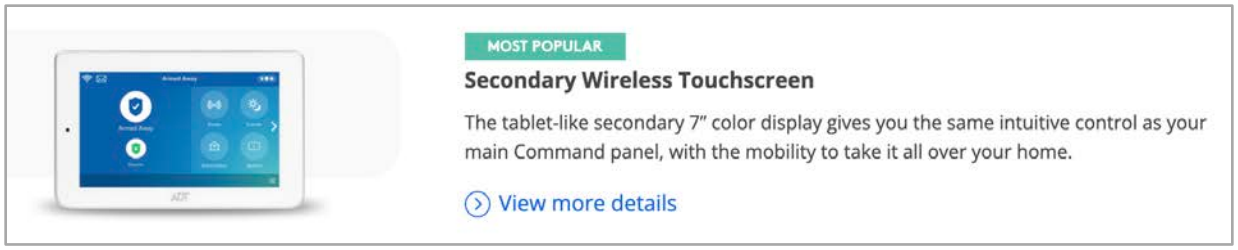


ADT Command, ADT, https://www.adt.com/command (last visited Oct. 5, 2022).



How to configure Wi-Fi on your ADT Command panel, YOUTUBE, https://www.youtube.com/watch?app=desktop&v=ZjNP95AeMZ4 (last visited Oct. 5, 2022).





Smart Home, ADT, https://www.adt.com/shop/packages/smart-home.html (last visited Oct. 5, 2022).

40. As shown above, the Accused Products provide easily configurable Wi-Fi settings. This capability ascertains the presence of a MAC controller and a Wi-Fi antenna and transceiver in the device and provides a secure wireless LAN.

41. The Accused Products further utilize a cryptography circuit that implements the 802.11 protocols authentication techniques, including, for example, TKIP and/or CCMP. Shown below is a block diagram from the 802.11 protocol documentation showing the TKIP-based cryptography circuit (such as used with WPA) that is utilized in the Accused Products. The circuit shown encrypts both address (destination address (DA), source address (SA)) and data information (plaintext MSDU) by adding encryptions bits (MIC key) to both the address and data. The cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1.1 TKIP cryptographic encapsulation

TKIP enhances the WEP cryptographic encapsulation with several additional functions, as depicted in Figure 8-4.

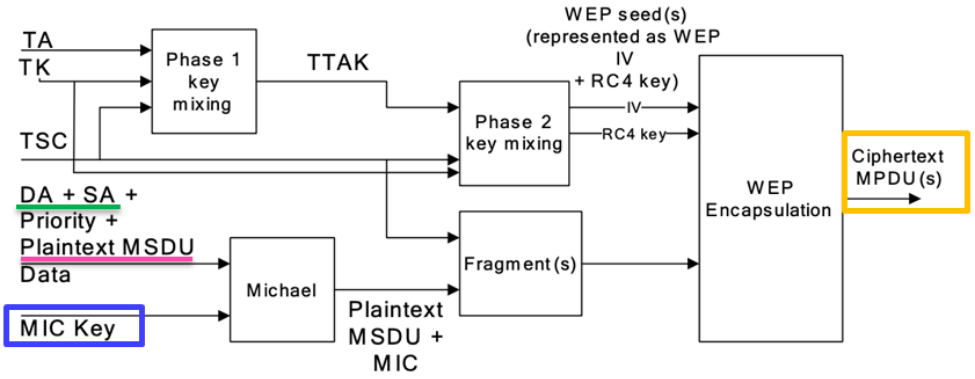


Figure 8-4—TKIP encapsulation block diagram

a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to appending the MIC.

b) If needed, IEEE Std 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU have the same value of extended IV (see 8.3.2.2).

c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed.

d) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with each MPDU to WEP for generation of the ICV (see 7.1.3.6), and for encryption of the plaintext MPDU, including all or part of the MIC, if present. WEP uses the WEP seed as a WEP default key, identified by a key identifier associated with the temporal key.

Page 213, 214, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

42. Shown below is a block diagram from the 802.11 protocol documentation showing the CCMP-based cryptography circuit (such as used with WPA2) that is utilized in the Accused Products. The circuit shown encrypts both address (A2 – MPDU address 2) and data information (plaintext MPDU) by adding encryptions bits (temporal key (TK)) to both the address and data. The cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.3.3 CCMP cryptographic encapsulation

The CCMP cryptographic encapsulation process is depicted in Figure 8-16.

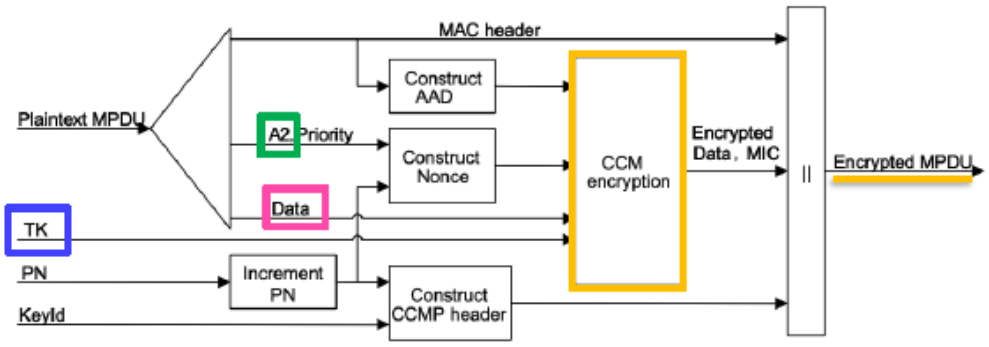


Figure 8-16—CCMP encapsulation block diagram

CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:

a) Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key. Note that retransmitted MPDUs are not modified on retransmission.

b) Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 when calculating the AAD.

c) Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2.

d) Place the new PN and the key identifier into the 8-octet CCMP header.

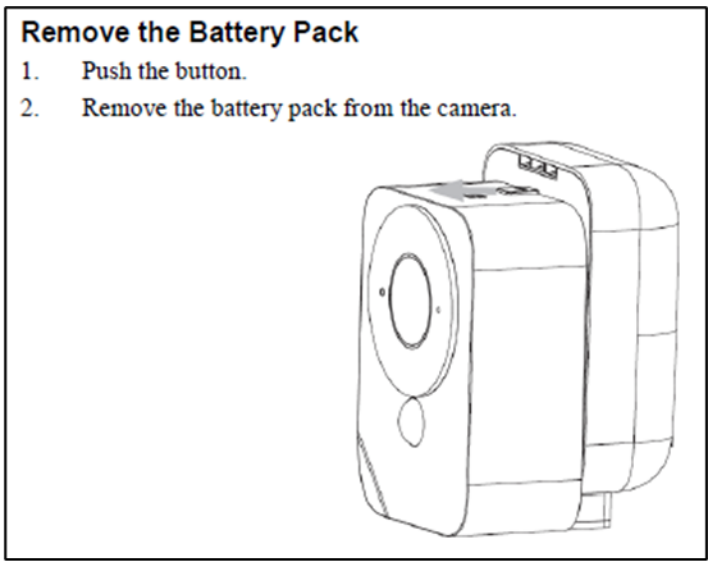
e) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing.

f) Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and MIC, as described in 8.3.3.2.

Page 229, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

43. Defendants also infringe the ’126 patent via products that utilize a volatile memory for storing cryptography information utilized in the cryptography circuit and a battery for maintaining the cryptography in the volatile memory. As shown in the set-up guide of Blue by ADT | Wireless Outdoor Cameras, model no. SCE2R0-29, submitted to the FCC, the camera utilizes a battery that provides power to maintain data, including cryptographic information in the

product's internal (volatile) memory. Such cryptographic information allows data encryption to be carried out over a secure wireless 802.11 network.

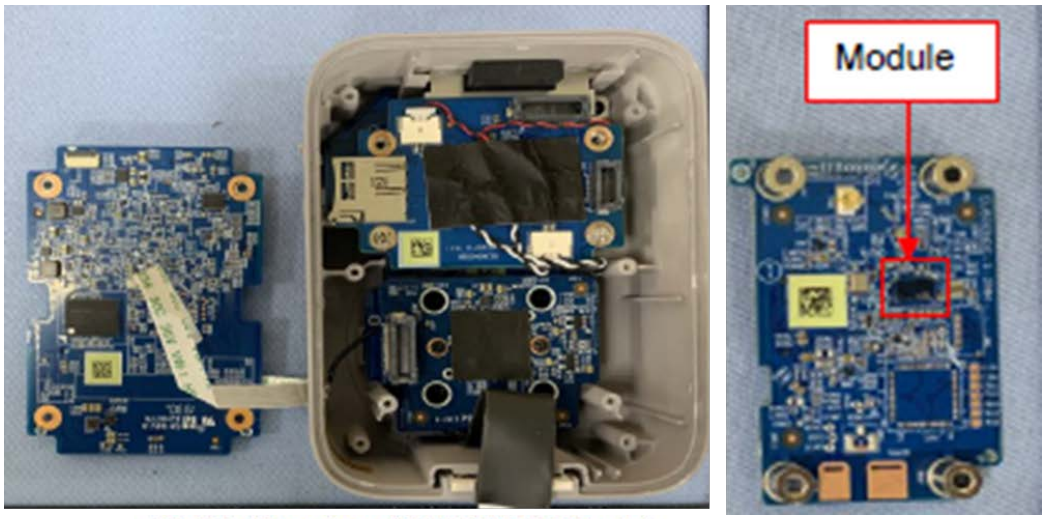


SCE2R0-29 Battery Camera

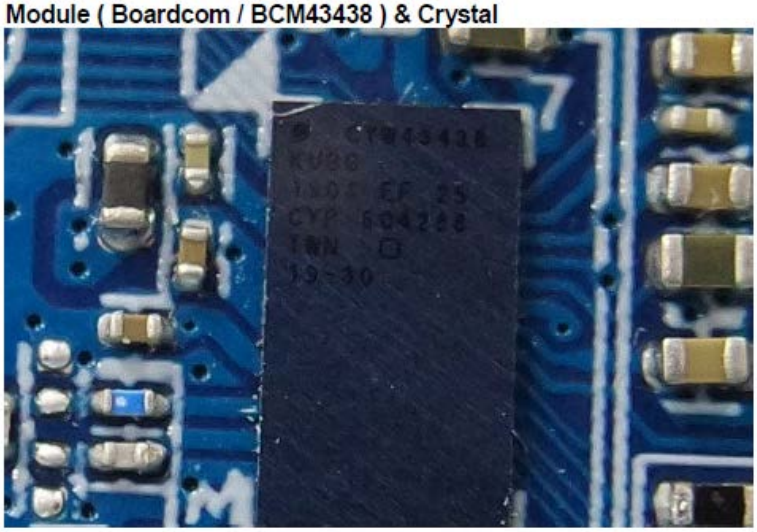
Model	SCE2R0-29
Network Interface	IEEE 802.11b/g/n
Battery (C1-04)	1, Minimum capacity 6140 mAh (22.2Wh)

See SCE2R0-29 Outdoor Camera | Setup Guide, accessible as a pdf file at https://fccid.io/P27SCE2R0 (submitted to the FCC, excerpts from cover page and pages 5-6, and 9) (last visited Dec. 16, 2022).

44. Furthermore, as shown below in pictures of a teardown of ADT's Outdoor Camera, model no. SCE2R0-29, the camera includes a Wi-Fi "module" (e.g., a "Broadcom/ BCM43438" model) that has an internal volatile memory for storing data, including cryptographic information.



Module (Boardcom / BCM43438) & Crystal



See Internal Photos of EUT, accessible as a pdf file at https://fccid.io/P27SCE2R0 (submitted to the FCC, excerpts from *Internal Photo.pdf*) (last visited Dec. 19, 2022).

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 7,224,678)

45. Plaintiff incorporates paragraphs 1 through 44 herein by reference.

46. Plaintiff is the assignee of the ’678 patent, entitled “Wireless local or metropolitan area network with intrusion detection features and related methods,” with ownership of all substantial rights in the ’678 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

47. The ’678 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ’678 patent issued from U.S. Patent Application No. 10/217,042.

48. ADT has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’678 patent in this District and elsewhere in Texas and the United States.

49. On information and belief, ADT designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of ADT and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants ADT Inc. and ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT.

50. Defendants each directly infringe the ’678 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the ’678 patent to, for example, their alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. Furthermore, on information and belief, Defendants each design the Accused Products for U.S. consumers, have made and/or sold and/or continue to make and/or sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, customers and/or other related service providers in the United States, or in the case that Defendants deliver the Accused Products outside of the United States they do so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby

directly infringing the ’678 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)”).

51. Furthermore, ADT Inc. directly infringes the ’678 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant ADT LLC, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Defendants. Defendants design the Accused Products for U.S. consumers, sell and offer for sale those Accused Products in the U.S. directly and to its related entities, and import the Accused Products into the United States for its related entities. On information and belief, U.S.-based subsidiaries, including at least ADT LLC, conduct activities that constitute direct infringement of the ’678 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. Defendant ADT Inc. is vicariously liable for the infringing conduct of Defendant ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT (under both the alter ego and agency theories). On information and belief, Defendants ADT Inc. and ADT LLC and U.S.-based subsidiaries members, segments, companies and/or brands of ADT are essentially the same company, comprising members, segments, companies and/or brands of ADT. Moreover, ADT Inc., as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

52. For example, ADT infringes claim 51 of the ’678 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to, ADT Doorbell Cameras, ADT Outdoor Security Cameras, ADT Indoor Security Cameras, ADT Command Panels, ADT Secondary Wireless Touchscreens, Blue by ADT Doorbell Cameras, Blue by ADT Wireless Outdoor Cameras, Blue by ADT Indoor Cameras, ADT SoSecure apps, ADT Control apps, ADT Pulse apps, and related accessories and software.

53. Those Accused Products include “[a]n intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations” comprising the limitations of claim 51. The technology discussion above and the example Accused Products provide context for Plaintiff’s allegations that each of those limitations are met. For example, the Accused Products include the steps of transmitting data between the plurality of stations using a media access layer (MAC), each of the stations having a respective MAC address associated therewith; monitoring transmissions among the plurality of stations to detect failed attempts to authenticate MAC addresses; and generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address.

54. At a minimum, ADT has known of the ’678 patent at least as early as the filing date of this complaint. In addition, ADT has known about its infringement of the L3Harris (“Harris”) patent portfolio, which includes the ’678 patent, since at least its receipt of a letter from Acacia Research Corporation, on behalf of Stingray, a subsidiary of Acacia Research Group, to ADT Security Services dated July 9, 2020, requesting ADT to discuss licensing the patent portfolio including the ’678 patent.

55. On information and belief, since at least the above-mentioned date when ADT was on notice of its infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b),

importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and other related service providers that make, import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '678 patent to directly infringe one or more claims of the '678 patent by making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date and/or dates of notice referenced above, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '678 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, and other related service providers through at least, *inter alia*, the following activities: creating advertisements that promote the infringing use of the Accused Products; creating and/or maintaining established distribution channels for the Accused Products into and within the United States; manufacturing and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products to purchasers and prospective buyers; testing wireless networking features in the Accused Products; and providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *OUR SERVICES*, ADT.COM, https://www.adt.com/services (last visited Oct. 7, 2022) (providing consumers with "Free in-home consultation," "Expert installation & repairs," and "Personal customer support"); *see also ADT*, YOUTUBE.COM, https://www.youtube.com/c/adt (providing consumers with ADT-produced how-to videos related to ADT products) (last visited Oct. 7, 2022). Furthermore, ADT markets and offers smartphone and tablet interfaces and its application software (e.g., apps) to provide access to the Accused Products, connect such products to wireless networks,

including Wi-Fi networks, provide remote control for ADT products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to control ADT products with voice commands or connect with other connected products. *See Apps for your mobile lifestyle*, ADT.COM, https://www.adt.com/apps (last visited Oct. 6, 2022) (showing ADT SoSecure app, ADT Control app, indicating that ADT apps enable integration with smart home platforms, and noting integration of Google Assistant-enabled Google Nest Mini with the ADT system enables voice commands of security, locks, lights, music and more); *ADT PULSE APP*, ADT.COM, https://www.adt.com/pulse (last visited Oct. 6, 2022) (stating "ADT Pulse works with your favorite devices" and showing logos for "Hey Google" and "amazon alexa"). Such compatibility provides convenience and added functionality that induces consumers to use ADT products, including at least the smartphone and tablet Wi-Fi interfaces utilizing WiFi apps and other protocols in networks with other third-party devices, and thus further infringe the '678 patent.

56. On information and belief, despite having knowledge of the patent portfolio including the '678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the portfolio, ADT has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the '678 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

57. Plaintiff Stingray has been damaged as a result of ADT's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an

amount that adequately compensates Stingray for ADT's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 7,440,572)

58. Plaintiff incorporates paragraphs 1 through 57 herein by reference.

59. Plaintiff is the assignee of the '572 patent, entitled "Secure wireless LAN device and associated methods," with ownership of all substantial rights in the '572 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

60. The '572 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '572 patent issued from U.S. Patent Application No. 09/760,619.

61. ADT has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '572 patent in this District and elsewhere in Texas and the United States.

62. On information and belief, ADT designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of ADT and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants ADT Inc. and ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT.

63. Defendants each directly infringe the '572 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '572 patent to, for example, their alter egos, agents, intermediaries, related entities, distributors, dealers,

importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. Furthermore, on information and belief, Defendants each design the Accused Products for U.S. consumers, have made and/or sold and/or continue to make and/or sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, customers and/or other related service providers in the United States, or in the case that Defendants deliver the Accused Products outside of the United States they do so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '572 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

64. Furthermore, ADT Inc. directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant ADT LLC, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Defendants. Defendants design the Accused Products for U.S. consumers, sell and offer for sale those Accused Products in the U.S. directly and to its related entities, and import the Accused Products into the United States for its related entities. On information and belief, U.S.-based subsidiaries, members, segments, companies and/or brands of ADT, including at least ADT LLC, conduct activities that constitute direct infringement of the '572 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. Defendant ADT Inc. is vicariously liable for the infringing

conduct of Defendant ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT (under both the alter ego and agency theories). On information and belief, Defendants ADT Inc. and ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT are essentially the same company, comprising members, segments, companies and/or brands of ADT. Moreover, ADT Inc., as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

65. For example, ADT infringes claim 1 of the ’572 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to, ADT Doorbell Cameras, ADT Outdoor Security Cameras, ADT Indoor Security Cameras, ADT Command Panels, ADT Secondary Wireless Touchscreens, Blue by ADT Doorbell Cameras, Blue by ADT Wireless Outdoor Cameras, Blue by ADT Indoor Cameras, ADT SoSecure apps, ADT Control apps, ADT Pulse apps, and related accessories and software.

66. Those Accused Products include “[a] secure wireless local area network (LAN) device” comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff’s allegations that each of those limitations are met. For example, the Accused Products include a housing; a wireless transceiver carried by said housing; a medium access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits to both the address and the data information, and for decrypting both the address and the data information upon reception.

67. ADT further infringes the ’572 patent via 35 U.S.C. § 271(g) by selling, offering to sell, and/or importing IoT and smart home devices, their components, and/or products containing same, that are made by a process covered by the ’572 patent. On information and belief, the infringing IoT and smart home devices, their components, and/or products containing same are not materially changed by subsequent processes, and they are neither trivial nor nonessential components of another product.

68. ADT further infringes based on the importation, sale, offer for sale, or use of the Accused Products that are made from a process covered by the ’572 patent. To the extent that Plaintiff made reasonable efforts to determine whether the patented processes of the ’572 patent were used in the production of the Accused Products but was not able to so determine, the Accused Products should be presumed by this Court to have been so made, pursuant to 35 U.S.C. § 295.

69. At a minimum, ADT has known of the ’572 patent at least as early as the filing date of this complaint. In addition, ADT has known about its infringement of the L3Harris (“Harris”) patent portfolio, which includes the ‘572 patent, since at least its receipt of a letter from Acacia Research Corporation, on behalf of Stingray, a subsidiary of Acacia Research Group, to ADT Security Services dated July 9, 2020, requesting ADT to discuss licensing the patent portfolio including the ’572 patent.

70. On information and belief, since at least the above-mentioned date when ADT was on notice of its infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and other related service providers that make, import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the ’572 patent to directly infringe one or more claims of the ’572 patent by

making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date of notice referenced above, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '572 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, and other related service providers through at least, *inter alia*, the following activities: creating advertisements that promote the infringing use of the Accused Products; creating and/or maintaining established distribution channels for the Accused Products into and within the United States; manufacturing and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products to purchasers and prospective buyers; testing wireless networking features in the Accused Products; and providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *OUR SERVICES*, ADT.COM, https://www.adt.com/services (last visited Oct. 7, 2022) (providing consumers with "Free in-home consultation," "Expert installation & repairs," and "Personal customer support"); *see also ADT*, YOUTUBE.COM, https://www.youtube.com/c/adt (providing consumers with ADT-produced how-to videos related to ADT products) (last visited Oct. 7, 2022). Furthermore, ADT markets and offers smartphone and tablet interfaces and its application software (e.g., apps) to provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi networks, provide remote control for ADT products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to control ADT products with voice commands or connect with other connected products. *See Apps for your mobile lifestyle*, ADT.COM,

https://www.adt.com/apps (last visited Oct. 6, 2022) (showing ADT SoSecure app, ADT Control app, indicating that ADT apps enable integration with smart home platforms, and noting integration of Google Assistant-enabled Google Nest Mini with the ADT system enables voice commands of security, locks, lights, music and more); *ADT PULSE APP*, ADT.COM, https://www.adt.com/pulse (last visited Oct. 6, 2022) (stating "ADT Pulse works with your favorite devices" and showing logos for "Hey Google" and "amazon alexa"). Such compatibility provides convenience and added functionality that induces consumers to use ADT products, including at least the smartphone and tablet Wi-Fi apps and other interfaces utilizing WiFi protocols in networks with other third-party devices, and thus further infringe the '572 patent.

71. On information and belief, despite having knowledge of the patent portfolio including the '572 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the portfolio, ADT has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the '572 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

72. Plaintiff Stingray has been damaged as a result of ADT's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for ADT's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 7,441,126)

73. Plaintiff incorporates paragraphs 1 through 72 herein by reference.

74. Plaintiff is the assignee of the ’126 patent, entitled “Secure wireless LAN device including tamper resistant feature and associated method,” with ownership of all substantial rights in the ’126 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements

75. The ’126 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ’126 patent issued from U.S. Patent Application No. 09/761,173 filed on January 16, 2001.

76. ADT has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’126 patent in this District and elsewhere in Texas and the United States.

77. On information and belief, ADT designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of ADT and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants ADT Inc. and ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT.

78. Defendants each directly infringe the ’126 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the ’126 patent to, for example, their alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. Furthermore, on information and belief, Defendants each design the Accused Products

for U.S. consumers, have made and/or sold and/or continue to make and/or sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, customers and/or other related service providers in the United States, or in the case that Defendants deliver the Accused Products outside of the United States they do so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '126 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

79. Furthermore, ADT Inc. directly infringes the '126 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant ADT LLC, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Defendants. Defendants design the Accused Products for U.S. consumers, sell and offer for sale those Accused Products in the U.S. directly and to its related entities, and import the Accused Products into the United States for its related entities. On information and belief, U.S.-based subsidiaries, members, segments, companies and/or brands of ADT, including at least ADT LLC, conduct activities that constitute direct infringement of the '126 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. Defendant ADT Inc. is vicariously liable for the infringing conduct of Defendant ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT (under both the alter ego and agency theories). On information and belief,

Defendants ADT Inc. and ADT LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of ADT are essentially the same company, comprising members, segments, companies and/or brands of ADT. Moreover, ADT Inc., as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

80. For example, Defendants infringe claim 1 of the ’126 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to Defendants’ infringing Accused Products that are enabled or compliant with Wi-Fi and that utilize a battery and a volatile memory for the storage of device data, including cryptographic data. Such Accused Products include, but are not limited to, security touchscreens (e.g., ADT’s Secondary Wireless Touchscreen) and security cameras (e.g., Blue by ADT |Wireless Outdoor Camera and Blue by ADT | Indoor Camera).

81. Those Accused Products include “[a] secure wireless local area network (LAN) device” comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff’s allegations that each of those limitations are met. For example, the Accused Products include a housing; a wireless transceiver carried by said housing; a media access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit comprising at least one volatile memory for storing the cryptography information, and a battery for maintaining the cryptography information in said at least one volatile memory.

82. At a minimum, ADT has known of the ’126 patent at least as early as the filing date of this complaint. In addition, ADT has known about its infringement of the L3Harris (“Harris”)

patent portfolio, which includes the '126 patent, since at least its receipt of a letter from Acacia Research Corporation, on behalf of Stingray, a subsidiary of Acacia Research Group, to ADT Security Services dated July 9, 2020, requesting ADT to discuss licensing the patent portfolio including the '126 patent.

83. On information and belief, since at least the above-mentioned date when ADT was on notice of its infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and other related service providers that make, import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '126 patent to directly infringe one or more claims of the '126 patent by making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date of notice referenced above, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '126 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, and other related service providers through at least, *inter alia*, the following activities: creating advertisements that promote the infringing use of the Accused Products; creating and/or maintaining established distribution channels for the Accused Products into and within the United States; manufacturing and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products to purchasers and prospective buyers; testing wireless networking features in the Accused Products; and providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *OUR*

SERVICES, ADT.COM, https://www.adt.com/services (last visited Oct. 7, 2022) (providing consumers with "Free in-home consultation," "Expert installation & repairs," and "Personal customer support"); *see also ADT*, YOUTUBE.COM, https://www.youtube.com/c/adt (providing consumers with ADT-produced how-to videos related to ADT products) (last visited Oct. 7, 2022). Furthermore, ADT markets and offers smartphone and tablet interfaces and its application software (e.g., apps) to provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi networks, provide remote control for ADT products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to control ADT products with voice commands or connect with other connected products. *See Apps for your mobile lifestyle*, ADT.COM, https://www.adt.com/apps (last visited Oct. 6, 2022) (showing ADT SoSecure app, ADT Control app, indicating that ADT apps enable integration with smart home platforms, and noting integration of Google Assistant-enabled Google Nest Mini with the ADT system enables voice commands of security, locks, lights, music and more); *ADT PULSE APP*, ADT.COM, https://www.adt.com/pulse (last visited Oct. 6, 2022) (stating "ADT Pulse works with your favorite devices" and showing logos for "Hey Google" and "amazon alexa"). Such compatibility provides convenience and added functionality that induces consumers to use ADT products, including at least the smartphone and tablet Wi-Fi apps and other interfaces utilizing WiFi protocols in networks with other third-party devices, and thus further infringe the '126 patent.

84. On information and belief, despite having knowledge of the patent portfolio including the '126 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the portfolio, ADT has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the

'126 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

85. Plaintiff Stingray has been damaged as a result of ADT's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for ADT's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

86. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

87. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

88. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

89. Plaintiff requests that the Court find in its favor and against Defendants, and that the Court grant Plaintiff the following relief:

a. A judgment that Defendants have infringed the Asserted Patents as alleged herein,

directly and/or indirectly by way of inducing infringement of such patents;

b. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;

c. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;

d. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;

e. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and

f. Such other and further relief as the Court deems just and equitable.

Dated: March 6, 2023

Respectfully submitted,

/s/ Jeffrey R. Bragalone __
Jeffrey R. Bragalone (lead attorney)
Texas Bar No. 02855775
E-mail: jbragalone@bosfirm.com
Terry A. Saad
Texas Bar No. 24066015
E-mail: tsaad@bosfirm.com
Marcus Benavides
Texas Bar No. 24035574
E-mail: mbenavides@bosfirm.com
Brandon V. Zuniga
Texas Bar no. 24088720
E-mail: bzuniga@bosfirm.com
BRAGALONE OLEJKO SAAD PC
901 Main Street
Suite 3800
Dallas, Texas 75202
Telephone: (214) 785-6670
Facsimile: (214) 785-6680

Wesley Hill
Texas Bar No. 24032294
E-mail: wh@wsfirm.com
WARD, SMITH, & HILL, PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
Telephone: (903) 757-6400
Facsimile: (903) 757-2323

ATTORNEYS FOR PLAINTIFF
STINGRAY IP SOLUTIONS LLC

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing PLAINTIFF'S SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT was filed electronically in compliance with Local Rule CV-5(a). Therefore, this document was served on all counsel who are deemed to have consented to electronic service on March 6, 2023.

/s/ *Jeffrey R. Bragalone*
JEFFREY R. BRAGALONE